

EXHIBIT R

How Mexico became the largest user of the world's best-known espionage program

An investigation by the Times reveals how the country became the most prolific user of Pegasus. He still uses it, despite the fact that the government promised to stop spying.



by **Natalie Kitroeff** and **Ronen Bergman**

Natalie Kitroeff reported this article from Mexico City and Ronen Bergman, from Tel Aviv.

April 18, 2023

The Israelis had come to Mexico to close an important sale: the Mexican army was about to become the first customer to buy their product, the most advanced spy program in the world.

But before they could close the deal, a discussion broke out about the price and speed of delivery of the espionage tool. The Mexican general who supervised the negotiations asked for a pause until the evening, according to two people who were present at the talks and a third who knows how the negotiations went.

The Times A weekly selection of stories in Spanish that you won't find anywhere else, with stories and accents. [Get it sent to your inbox.](#)

"We will pick them up at your hotel and make sure there is a better atmosphere," they remember that the general said.

That night, a group of cars arrived at the Israeli executives' hotel and moved them to a new place for crucial negotiations: a striptease club in the heart of Mexico City.

The general's security team ordered the rest of the clientele to leave the club, according to the three people who know the negotiations, and the talks resumed.

It was in March 2011, in that dark cabaret where women danced on stage and between drinks of tequila, where the use of the most powerful cybernetic weapon that exists was conceived.

The spy program, known as Pegasus, has since become a global synonym for the chilling scope of state surveillance. From Europe to the Middle East, governments have used that tool to hack thousands of mobile phones.

No place has had more experience with the capabilities and dangers of this technology than Mexico, the country that inaugurated its dissemination around the world.

An investigation by The New York Times based on interviews, documents and forensic evidence of *hacked* phones shows the secret exchanges that made Mexico the first customer of Pegasus, and also reveals that the country became the most prolific user of the best-known spy program in the world.

Mexico began to use the surveillance tool against civilians who were facing the State, abuses that the country insists on having stopped. But the Times discovered that Mexico continues to use Pegasus to spy on people who defend human rights, even in recent months.



The president of Mexico, Andrés Manuel López Obrador, who took office in 2018, promised to stop the espionage practices of the past, which he described as "illegal." Luis Antonio Rojas for The New York Times

Many tools can infiltrate your digital life, but Pegasus is exceptionally powerful. It can infect your phone without any sign of intrusion and extract everything it has - every email, text message, photo, calendar appointment - while monitoring everything you do with the device, in real time.

You can record all keyboard taps, even when using encrypted applications, and monitor through the phone's camera or listen through your microphone, even if the device seems to be turned off.

The program has been used to fight crime, helping to dismantle networks of abuse of minors and arrest famous figures, such as Joaquín Guzmán Loera, the drug trafficker known as El Chapo.

But, again and again, Pegasus has also been used illegally by governments in order to spy on and repress human rights defenders, democracy activists, journalists and other citizens who challenge corruption and abuse.

Alarmed by the use of Pegasus to "miciously attack" dissidents around the world, in 2021 the Biden government blacklisted NSO Group, the Israeli company that makes the spy program.

Shortly after, the Israeli Ministry of Defense - which must approve the export of Pegasus to other countries - said that it would prohibit sales to nations where there is a risk of human rights violations.

However, despite the numerous evidence of Pegasus' abuses in Mexico, the Israeli government has not ordered its use to end in the country, according to four people who know the contracts for the use of that technology.

In fact, according to those four people, the Mexican army is not only Pegasus' oldest client but has also attacked more mobile phones with that malicious program than any other government agency in the world.

In addition, the spy program is still used in the country, and not only to combat crime.

After the revelations of the use of Pegasus against government critics affected the management of his predecessor, President Andrés Manuel López Obrador, who took office in 2018, promised to stop the espionage practices of the past, which he described as "illegal."

But he didn't. Evidence that had not been revealed so far shows that, as recently as the second half of 2022, Pegasus infiltrated the cell phones of two of the country's main human rights defenders, who provide legal representation to the victims of one of the most serious mass disappearances in Mexico's history.



A military patrol unit in Michoacán, Mexico. The Mexican army has used a spy program to track down leaders of the drug cartels, but it has also used it to spy on human rights defenders, according to an investigation by the Times. Daniel Berehulak for The New York Times

The army has a history of human rights abuses and its role in that disappearance has been one of the focuses of the investigation for years. And, as new accusations have appeared against the military in the case in the last year, both defenders were repeatedly targeted by Pegasus, according to forensic evidence carried out by Citizen Lab, a research institute based at the University of Toronto.

The Mexican army is the only entity in the country that currently operates Pegasus, according to the four people familiar with the contracts.

The Israeli Ministry of Defense did not want to comment. The Ministry of National Defense of Mexico did not want to talk about the recent hack, but said that it followed the government's position, which affirms that the procedures for collecting intelligence information are "in no way aimed" at invading the private lives of political, civic and media personalities.

This is the second wave of attacks on the phone of Santiago Aguirre, one of the human rights defenders. He had also been the target of Pegasus during the previous government, according to Citizen Lab.

"In this government, so many promises were made that things were going to be different," Aguirre said. "Our first reaction was like saying: 'It can't be that we are in the same thing *again*.'"

A spokesman for the Mexican president declined to comment. In a statement, NSO Group said that "it adheres to strict regulation and cannot reveal the identity of its customers." The company questioned the forcefulness of Citizen Lab's forensic analyses, while the organization said it had no doubts about its conclusions.

To verify if Pegasus hacked the two Mexican defenders in recent months, NSO Group said it would need to be "accessed to the data." But the defenders said they were not willing to give the government espionage partner more private information.

For a long time, the beginnings of the use of Pegasus in Mexico have been surrounded by secrecy. After the night at the striptease club, the Israeli executives of NSO Group, which was then a start-up company, returned to Tel Aviv with the general guidelines of their first sale. The next step was a contract itself.



President Biden with López Obrador in January. The Biden government blacklisted NSO Group, the Israeli company that manufactures the spy program. Doug Mills/The New York Times

So, a few months later, a team of NSO representatives returned to Mexico to give demonstrations of the spy program to some of the most powerful people in the country.

On May 25, 2011, Eran Reshef, an Israeli executive of the defense industry who helped negotiate the agreement, said in an email to the president of NSO and its two founders that "the demonstration to the Secretary of Defense and the president will be made next Friday," referring to the president of that time, Felipe Calderón, and his Secretary of Defense, Guillermo Galván Galván. A copy of the email was filed in an Israeli lawsuit for the commissions of the sale of Pegasus to Mexico.

Two of the people who attended the demonstration said that it took place in an extensive military base located on the edge of Mexico City, where the first Pegasus machine would be installed.

For fear of leaks, the Mexican army made Israeli executives wait in a tiny room where the cleaning items were stored, so that no one would see them before making their presentation. An armed soldier was stationed in front of the door.

When Calderón and Galván Galván arrived, they sat in front of the large screens on the wall and watched a phone be hacked, according to the attendees.

Udi Doenyas, chief technology officer of NSO Group, who invented the Pegasus architecture and led the team that wrote the code for the first version of the spy program, confirmed that he connected the system to a screen and handed over a BlackBerry phone to senior Mexican officials. Then he asked them to use it.

While using it, the phone showed no signs of being at risk, but the Pegasus system began to methodically extract all the data and transmit it to the screen for everyone to see.

This was the superpower of the spy program: the stealth attack.

Miguel Ángel Sosa, Calderón's spokesman, acknowledged that the former president visited the facilities of the Ministry of Defense, where "various presentations were made about the tasks" that were being carried out, "including the collection of information and intelligence."

But he also said that Calderón was never informed if they finally bought the spy program, and that the former president was never told - "nor this inquiry" - what means were used to capture the criminals.



President Felipe Calderón and his Secretary of Defense, Guillermo Galván Galván, in 2009. Dario Lopez-

Mills/Associated Press

At that time, Mexico urgently needed a reliable way to hack BlackBerry phones, one of the favorite devices of the country's fearsome drug cartels. Since the beginning of his mandate in 2006, Calderón had promoted the so-called boss's strategy to confront organized crime, focusing on the main leaders of criminal groups.

To locate the drug lords, a technology was needed that would allow the spies to have their location constantly. The criminals were cautious, explain the former officials of the security forces, moved from one side to the other and turned off their phones to avoid being captured.

"You didn't have time to mount the operation," said Guillermo Valdés, former director of CISEN, which was the equivalent of the CIA in the country, from 2007 to 2011.

At "the time he turned off the phone," Valdés said, "we no longer knew where he was."

Until that time, Mexico had been very dependent on the United States.

"The pressure on the army to improve its intelligence capabilities was intense," said Alejandro Hope, a former intelligence official during Calderón's government. He also explained that an attractive potential of Pegasus was that it would give Mexico its own system.

"They no longer wanted to depend on Americans," Hope said.

The army signed the contract to buy the spy program shortly after the demonstration.

In September 2011, about 30 NSO employees, most of the company's staff, flew to Mexico to install Pegasus, test it and instruct a team of about 30 Mexican soldiers and officers on how to operate the technology, according to three people familiar with the installation process. The Mexican unit chosen to operate it is called the Military Intelligence Center, a hermetic branch of the army of which there is little public information.

When the Mexicans were ready to handle Pegasus on their own, a brief ceremony was held in December as a way to "deliver the keys," said two of the people who know the details of the installation.

A 2019 document, which is part of the huge hacking of military emails in Mexico that took place last year, indicates that the intelligence center is housed in a horseshoe-shaped complex. Three people familiar with the facilities say that the commanders look through internal glass walls, while the information unfolds on huge screens.



A branch of the NSO Group near Saphir, IsraelCredit Amit Elkayam for The New York Times

In a 2021 document, which was also disclosed by the hack, the army says that one of the main risks faced by the center is "that the activities carried out in this center are evidenced to public opinion."

Pegasus was quickly adopted by the Mexican authorities, and after Enrique Peña Nieto assumed the presidency in 2012, two more government agencies bought it: the attorney general's office and CISEN, according to Mexican officials and three people who know the contracts.

In a few years, the spy program began to infiltrate the phones of some of Mexico's most prominent human rights lawyers, journalists and anti-corruption activists, a surveillance that moved away from the agreement with the Israelis to focus on serious crimes and terrorism.

Criticism was not long in coming, both in the country and abroad, and the scandal persecuted Peña Nieto for the rest of his presidency. Mexico has spent more than 60 million dollars on Pegasus, according to Mexican officials who referred to previous governments.

The Mexican army has recognized that it only had Pegasus between 2011 and 2013. But a group of independent experts investigating the disappearance of 43 students who planned to go to a protest claimed that the military had Pegasus when they were kidnapped in 2014, and that they were spying on the phones of people involved in the crime during the night the events

happened.

It is not clear why the military was spying, but intelligence was not used to help find the students, the experts said.

After López Obrador took office in 2018, he dissolved the federal police and replaced the Mexican espionage agency with a new entity.

From 2019 until today, only the military has had Pegasus, say four people with knowledge of the contracts. And during that time, the malicious program has continued to be used against journalists, human rights defenders and an opposition politician, according to Citizen Lab's analysis.

According to Mexican legislation, government entities need the authorization of a judge to spy on private communications. But in public statements, the army has not made any request to intervene in those communications in recent years.

On a Thursday afternoon last December, Aguirre received an email that looked like it was taken from a spy novel.



Santiago Aguirre, a human rights defender, has been repeatedly targeted by the Pegasus spy program.
Celia Talbot Tobin for The New York Times

"Apple believes that you are a target of state-sponsored attackers who are trying to remotely compromise the iPhone associated with their Apple ID," the message said, which was reviewed by the Times. "It is likely that these attackers are watching him, individually, for who he is or for what he does."

In 2021, Apple announced that it would start sending those warnings to users whose mobile phones had been hacked by sophisticated spyware. The email went on to say that "sensitive data" from Aguirre's phone could be compromised, "even the camera and microphone."

Years earlier, Aguirre, who is the executive director of the Miguel Agustín Pro Juárez Human Rights Center, had been the target of Pegasus.

His stomach was upset when he thought that government spies were reviewing his entire digital life, from messages with torture survivors to family photos with his young daughter.

Then he realized: others could also be in danger.

He ran down the corridor to the office of María Luisa Aguilar, the main defender who carries out the international work of the group. She had received the same email.

Both contacted the Mexican digital rights group known as R3D, which had their telephone data analyzed by Citizen Lab. He confirmed that both were hacked multiple times by Pegasus between June and September 2022.

"In the eyes of the armed forces, we represent a risk," Aguilar said. "They don't want to lose the power they have accumulated."

Natalie Kitroeff reported from Mexico City and Ronen Bergman, from Tel Aviv.

Natalie Kitroeff is the head of the Times correspondent for Mexico, Central America and the Caribbean. @Nataliekitro

Ronen Bergman is a *staff* reporter for The New York Times Magazine and lives in Tel Aviv. His most recent book is *Rise and Kill First: The Secret History of Israel's Targeted Assassinations*, published by Random House.